TOPICS

スマートフォンのリスク及びその対策について

独立行政法人情報処理推進機構
技術本部 セキュリティセンター 調査役
加賀谷 伸一郎

はじめに

ここ2、3年の間で、急速に普及が進んでいるスマートフォン。新しく発売される携帯電話はそのほとんどがスマートフォンであり、従来型携帯電話（フィーチャーフォンと呼ばれる場合もある）に取って代わろうという勢いです。スマートフォンは「電話機」ではありますが、その中身（機能）はほとんどパソコンと言っても過言ではありません。もう少し正確に表現するなら、「スマートフォン＝パソコン＋携帯電話（常時インターネット接続）＋システム手帳（電話帳やスケジュール帳など）」であり、従来型携帯電話およびパソコンよりも、さらに取り扱いに注意すべきものであると言えます。

しかしながら、実際は従来型携帯電話の延長という意識で扱われることが多く、その脅威が正しく理解されているとは言えません。そこで今回は、スマートフォンを取り巻く脅威の現状と対策について、解説していきます。

スマートフォンの特徴

従来型携帯電話と比較しながら、セキュリティ面におけるスマートフォンの特徴を解説します。国内の従来型携帯電話は、携帯電話会社毎に独自の通信網および独自の基本ソフト（OS）を使用していたため、アプリやサービスに互換性はありませんでした。さらに、アプリのインストールについて利用者の自由度が制限されていたこともあり、ウイルスの入り込む余地はほとんど無く、結果的にセキュリティは強固になっていました。こ

のため、悪意ある者によってウイルスが作成されることはありませんでした。しかしながら、独自の進化を遂げた日本の従来型携帯電話が「ガラパゴスケータイ」などと揶揄されることにもなったのは、皮肉なことです。

一方、スマートフォンは従来型携帯電話と異なり、基本ソフト（OS）やサービスが全世界的に共通の仕様であることに、注意が必要です。この点は、パソコンと状況が非常に良く似ています。すなわち、海外でウイルスが発生した場合、日本にいても感染する危険があるということです。このことからも、スマートフォンは、パソコンと同様の脅威にさらされているということを自覚すべきです。

さらにスマートフォンでは、アプリのインストールについて、従来型携帯電話と比較すると格段に自由度が高くなっています。アプリ開発についても、開発ツールが一般に公開されていることもあり、ソフトウェアの知識さえあれば、開発は容易になっています。そのため、スマートフォンは、パソコンと同様に、ウイルスなど悪意のあるプログラムに狙われやすい状況となっているのが実情です。（図）

ウイルス脅威の現状

2011年から、スマートフォン、特にアンドロイド端末を狙ったウイルスなど不正アプリが日本でも次々と発見されるようになりました。スマートフォンがウイルスに感染してしまった場合に想定される被害例として、以下が考えられます。

○スマートフォン内の電話帳、メールアドレス、位置情報など、個人情報など重要な情報が悪意ある第三者に送られてしまう。

○悪意ある第三者にスマートフォンを乗っ取られて、自由自在に操られてしまう。

これらの他、パソコンで起こり得るウイルス感染被害はそのほとんどがスマートフォンにおいても起こる可能性が高いという認識で、あながち間違いではありません。

被害の実情

日本で確認されている被害のほとんど全ては、アンドロイド端末に不正なアプリをインストールしてしまったというものです。不正アプリは、公式ではないマーケットサイトなどに置かれていることが多くなっています。不特定多数にばらまかれたメールに書かれた甘いうたい文句に釣られてURLリンクを押すと、不正アプリが置かれているサイトに誘導されてしまいます。そして、不正アプリのファイルをダウンロードし、インストールしてしまうのです。現在、日本で流通している不正アプリのほとんどは、スマートフォン内の電話帳の内容を盗むものです。

つまり、自分の友人や知人の個人情報が悪用されてしまう可能性があるのです。不正アプリを取り込んでしまわないように、注意しましょう。

スマートフォンを安全に使用するための六箇条

以前からパソコンを使ってきた人であれば、スマートフォンにおける脅威も比較的容易に理解できるでしょう。

しかしながら、特に若年層においてはパソコンの利用経験が浅いまま、従来型携帯電話からスマートフォンに移行した人がほとんどであり、脅威に対して知識も免疫も全く無いと言っても過言ではありません。つまり、スマートフォン利用者に対して、脅威についての知識を与え、パソコンと同様の対策を呼びかけることは急務と言えます。

情報処理推進機構（IPA）では、スマートフォン利用者に向けた注意喚起情報を発信するとともに、「スマートフォンを安全に使用するための六箇条」を発表しています。

各項目について以下に詳しく説明していきます。

【1】スマートフォンをアップデートする

販売元からOSのアップデートが提供された場合、直ちにアップデートしましょう。アップデートをしないで使っていると、パソコン同様、脆弱性（ぜいじゃくせい）を悪用した攻撃に遭う危険性が高まります。またその際、アップデート手順をきちんと理解することが重要です。アップデート手順は、販売元や製造元によって異なる場合があります。きちんとアップデートするために、取扱説明書などを確認し、正しい手順を身につけたうえでアップデートを実践しましょう。また、アプリについても同様に、アップデートは重要です。

【2】スマートフォンにおける改造行為を行わない

ここでの改造行為とは、スマートフォンの安全性確保のための制限を取り外す行為で、例えばアイフォーンにおける「脱獄」やアンドロイド端末における「ルート権限奪取行為（ルート化とも呼ばれる）」などのことを指します。スマートフォンで動作するウイルスの中には、改造行為を行ったスマートフォンのみに感染するものも確認されています。ウイルス感染の危険性を自ら高めてしまうことになるため、スマートフォンの改造行為は絶対に行ってはなりません。

【3】信頼できる場所からアプリをインストールする

スマートフォンのアプリは、基本的に公式のマーケットサイトなどで入手しましょう。アイフォーンであれば米アップル社の「アップストア」、アンドロイド端末であればグーグル社の「グーグルプレイ」が公式マーケット／ストアです。

なお、アンドロイド端末の場合、「グーグルプレイ」でも不正アプリの流通が確認されたことがあるため、日本では、直接「グーグルプレイ」にアクセスするのではなく、まずは携帯電話会社が運営するマーケット（アプリ紹介サイト）にアクセスしてアプリを選ぶことを強くお勧めします。携帯電話会社が運営するマーケットでは、アプリのチェックなどにより、ウイルスなど不正アプリの排除を実施しているため、信頼性が高いのです。

【4】アンドロイド端末では、アプリをインストールする前に、アクセス許可を確認する

アンドロイド端末の場合、アプリをインストールする際に表示される「アクセス許可」（アプリがアンドロイド端末のどの情報／機能にアクセスするか定義したもの）の一覧には必ず目を通しましょう。

不正アプリは、電話帳など個人情報などを盗み取るために、アプリの種類から考えると不自然なアクセス許可をユーザーに求めることがあります。例えば、単なるゲームアプリにも関わらず、電話帳の内容へアクセスするための許可を求める、などです。

アンドロイド端末にアプリをインストールする際に、不自然なアクセス許可や疑問に思うアクセス許可を求められた場合には、そのアプリのインストールは中止すべきです。

【5】セキュリティソフト（アプリ）を導入する

スマートフォンの中でもアンドロイド端末では、2011年初頭以降、大手ウイルス対策ソフト開発会社が続々とセキュリティソフトを発売し、その選択肢は充実しています。アンドロイド端末では【4】に注意すればウイルスに感染する可能性を低減できますが、人によっては判断が難しい場合もあります。ウイルス感染の可能性をより低減するためにセキュリティアプリを導入しましょう。

【6】スマートフォンを小さなパソコンと考え、パソコンと同様に管理する

スマートフォンには個人情報やプライベート情報がたくさん詰まっています。第三者に勝手に見られたり操作されたりしないよう、暗証番号など「端末ロック」を設定することを心掛けましょう。自分になりすまされて、勝手にメールを送られてしまうなどの被害も防止できます。

スマートフォンを快適に利用していくためにも、以上の六箇条を必ず実践し、リスクを減らすよう、心掛けましょう。

1 スマートフォンをアップデートする。
2 スマートフォンにおける改造行為を行わない。
3 信頼できる場所からアプリケーション（アプリ）をインストールする。
4 アンドロイド端末では、アプリをインストールする前に、アクセス許可を確認する。
5 セキュリティソフトを導入する。
6 スマートフォンを小さなパソコンと考え、パソコンと同様に管理する。

PROFILE
加賀谷 伸一郎（かがや しんいちろう）
（IPA 技術本部 セキュリティセンター 調査役）
コンピュータウイルス・不正アクセスの届出受付、情報セキュリティ関連相談への対応および情報セキュリティ対策全般の普及啓発活動に従事。
1991年に株式会社東芝入社。2003年に社内分社で設立された東芝ソリューション株式会社に移り、情報セキュリティ関連ソリューション開発などに従事。
2004年10月よりIPA勤務。2007年7月にIPAに転籍。2011年9月より現職。